

UNITED STATES DISTRICT COURT

for the

Eastern District of California

FILED

Aug 05, 2022

CLERK, U.S. DISTRICT COURT  
EASTERN DISTRICT OF CALIFORNIA

In the Matter of the Search of )  
One Apple iPhone in a blue case bearing an )  
unknown serial number; )  
)  
One black Samsung LG cellular telephone )  
bearing an unknown serial number; )  
)  
One silver Apple iPhone in a clear case )  
bearing an unknown serial number; )  
)  
One black Samsung cellular telephone bearing )  
an unknown serial number; )  
)  
One silver and white Samsung cellular )  
telephone bearing an unknown serial number; )  
)  
One Microsoft Surface Pro tablet bearing )  
serial number JT2L416JA1C; and )  
)  
One white Samsung cellular telephone bearing )  
an unknown serial number; )  
)  
CURRENTLY LOCATED AT 2001 Freedom )  
Way, Roseville, California 95678 )

Case No. 2:22-sw-523-JDP

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

**SEE ATTACHMENT A, attached hereto and incorporated by reference.**

located in the \_\_\_\_\_ Eastern \_\_\_\_\_ District of \_\_\_\_\_ California \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

**SEE ATTACHMENT B, attached hereto and incorporated by reference.**

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

21 U.S.C. §§ 846, 841(a)(1)

Conspiracy to distribute and to possess with intent to distribute controlled substances

The application is based on these facts:

**SEE AFFIDAVIT and ATTACHMENT C, attached hereto and incorporated by reference.**

- ☐ Continued on the attached sheet.
- ☐ Delayed notice \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

\_\_\_\_\_  
/s/ Christopher Fitzpatrick

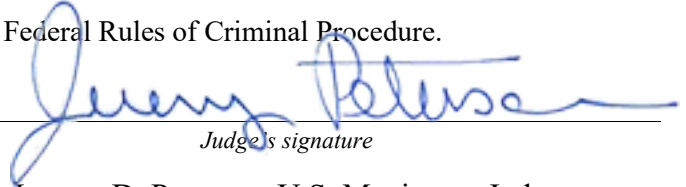
*Applicant's signature*

\_\_\_\_\_  
Christopher Fitzpatrick, IRS-CI Special Agent

*Printed name and title*

Sworn to and signed telephonically, consistent with Rule 4.1 of the Federal Rules of Criminal Procedure.

Date: August 5, 2022

\_\_\_\_\_  


*Judge's signature*

City and state: Sacramento, California

\_\_\_\_\_  
Jeremy D. Peterson, U.S. Magistrate Judge

*Printed name and title*

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

I, Christopher Fitzpatrick, being first duly sworn, hereby depose and state as follows:

**I. INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—multiple electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Internal Revenue Service-Criminal Investigations (“IRS-CI”), and have been since September 2001. I am currently assigned to the IRS-CI Sacramento Office, and I am charged with investigating drug trafficking and money laundering activities in the Eastern District of California, and elsewhere. I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and I am empowered by law to conduct investigations and make arrests for federal felony offenses. Additionally, I am a federal law enforcement officer within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure, that is, a federal law enforcement agent engaged in enforcing criminal laws and authorized to request a search warrant.

3. I was trained at the Federal Law Enforcement Training Center located in Glynco, Georgia. During my training, I received special training in money laundering, including but not limited to, 18 U.S.C. §§ 1956 and 1957, and 31 U.S.C. § 5324(a)(1). I also received special training in specified unlawful activities under the money laundering statutes, including but not limited to, violations of 21 U.S.C. §§ 846 and 841(a)(1). I have also spoken to and worked with experienced federal, state, and municipal agents and narcotics officers regarding the methods and means employed by drug manufacturers and drug traffickers, including their use of express carriers and the United States Postal Service (“USPS”) to distribute illegal narcotics.

4. I am part of the Northern California Illicit Digital Economy (“NCIDE”) Task Force composed of IRS-CI, Homeland Security Investigations, the Federal Bureau of Investigation (“FBI”), the United States Postal Inspection Service (“USPIS”), the United States

Postal Inspection Service-Office of the Inspector General (“USPIS-OIG”), and the Drug Enforcement Administration (“DEA”). As a function of this task force, investigators regularly purchase narcotics utilizing both digital and fiat currencies, from the persons operating and illegally selling narcotics on the “clear” portion of the internet, from the “dark” portion of the internet, and from various social media platforms. Investigators conduct the undercover purchases of narcotics to assist in the effort to identify the suspects operating such illicit sites.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Specifically, this affidavit incorporates facts communicated to me by other law enforcement officers.

## **II. IDENTIFICATION OF THE DEVICES TO BE EXAMINED**

6. The property to be searched (collectively, the “Subject Devices”) consists of the following:

- a) One Apple iPhone in a blue case bearing an unknown serial number (“Subject Device 1”);
- b) One black Samsung LG cellular telephone bearing an unknown serial number (“Subject Device 2”);
- c) One silver Apple iPhone in a clear case bearing an unknown serial number (“Subject Device 3”);
- d) One black Samsung cellular telephone bearing an unknown serial number (“Subject Device 4”);
- e) One silver and white Samsung cellular telephone bearing an unknown serial number (“Subject Device 5”);
- f) One Microsoft Surface Pro tablet bearing serial number JT2L416JA1C (“Subject Device 6”); and
- g) One white Samsung cellular telephone bearing an unknown serial number (“Subject Device 7”).

///

7. The Subject Devices are currently located at the FBI's Roseville field office at 2001 Freedom Way in Roseville, California, and specifically in the possession of the FBI's Computer Analysis and Response Team ("CART"). The applied-for warrant would authorize the forensic examination of the Subject Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

### **III. PROBABLE CAUSE**

8. Law enforcement is investigating conspiracies to distribute narcotics and launder the resulting proceeds that occurred on the dark web beginning as early as April 2021 and continuing until at least on or around March 29, 2022. Holly Adams and Devlin Hosner are charged by indictment as part of these conspiracies in the case filed in this judicial district and captioned *United States v. Holly Adams*, No. 2:22-cr-00100-JAM.

#### **A. Law Enforcement Seized the Subject Devices While Executing Search Warrants in the Central District of California.**

9. On or around March 29, 2022, law enforcement agents executed search warrants at Room 224 of the Indian Wells Resort Hotel in Indian Wells, California ("Room 224"), where Adams and Hosner were staying. These search warrants were approved by a United States Magistrate Judge for the Central District of California and numbered as follows:

- a) Search warrant number 5:22-mj-00193, which authorized law enforcement to seize and subsequently search any digital devices within Hosner's immediate vicinity and control at the location where the search warrant was executed;<sup>1</sup>
- b) Search warrant number 5:22-mj-00194, which authorized law enforcement to seize and subsequently search any digital devices within Adams's immediate vicinity and control at the location where the search warrant was executed;

///

---

<sup>1</sup> This affidavit incorporates by reference the facts stated in my affidavit in support of search warrant number 5:22-mj-00193, which is attached to the instant application as Attachment C. This same affidavit was submitted in support of search warrant numbers 5:22-mj-00194 and 5:22-mj-00196.

- c) Search warrant number 5:22-mj-00196, which authorized law enforcement to seize and subsequently search any digital device inside Room 224 which was itself or which contained evidence, contraband, fruits, or instrumentalities of narcotics trafficking and money laundering.

10. Consistent with the above authority, law enforcement agents seized the Subject Devices when they executed these search warrants at the Indian Wells Resort Hotel on March 29, 2022. Specifically, the Subject Devices came into law enforcement's possession in the following ways:

- a) Subject Device 1 was seized from Adams's person;
- b) Subject Device 2 was seized from the top of a bed located inside Room 224;
- c) Subject Device 3 was seized from the top of a bed located inside Room 224;
- d) Subject Device 4 was seized from a Michael Kors purse located inside Room 224;
- e) Subject Device 5 was seized from under a coffee table located on the floor of Room 224;
- f) Subject Device 6 was seized from a television stand located inside Room 224; and
- g) Subject Device 7 was seized from between the cushions of a couch located inside Room 224.

11. Each of the search warrants described above authorized law enforcement to complete searches of any seized digital devices within 120 days of the warrants' execution. Each of the search warrants described above also contained the following limitation: "The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court."

**B. The Subject Devices Are in FBI Custody in Roseville.**

12. On March 29, 2022, the Subject Devices were booked into evidence at the FBI field office located at 3480 Vine Street in Riverside, California. On April 4, 2022, the Subject Devices were transferred by FBI personnel to the FBI field office located in Roseville.

///

13. On April 5, 2022, the Subject Devices were received by the FBI field office located in Roseville and booked into evidence there. As of the date of this affidavit, the Subject Devices have not been removed from the secure evidence room of the FBI field office located in Roseville. Hence, based on the above facts and on my training and experience, I know that the Subject Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Subject Devices first came into law enforcement possession.

14. The 120-day examination period authorized by the three search warrants issued in the Central District of California expired on or around July 27, 2022. As of the date of this affidavit, FBI CART has not begun its examination of the Subject Devices due to a variety of factors, including staffing shortages and the effects of the global COVID-19 pandemic. Hence, the warrant I am applying for would re-authorize law enforcement to search for and seize the items described in Attachment B, but to do so beyond the 120-day window previously authorized by the Central District of California.

#### **IV. TECHNICAL TERMS**

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a) Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still

photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b) Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c) Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d) GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved



in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e) PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f) IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control

a range of IP addresses. Some computers have static or long-term-IP addresses, while other computers have dynamic or frequently changed IP addresses.

- g) Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

16. Based on my training, experience, and research, I know that the Subject Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs. Furthermore, in my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

#### **V. ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. There is probable cause to believe that things that were once stored on the Subject Devices may still be stored there, for at least the following reasons:

- a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

**A. Forensic Evidence**

19. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Devices because:

- a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers,

email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b) Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d) The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

///

///

**B. Nature of Examination**

20. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for would permit the examination of the Subject Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

**C. Manner of Execution**

21. Because this warrant seeks only permission to examine electronic devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

**VI. CONCLUSION**

22. I submit that this affidavit establishes probable cause for a search warrant authorizing the examination of the Subject Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

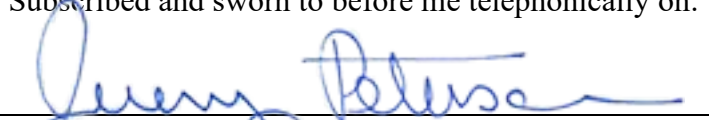
/s Christopher Fitzpatrick

Christopher Fitzpatrick

Special Agent

Internal Revenue Service-Criminal Investigations

Subscribed and sworn to before me telephonically on: August 5, 2022



THE HONORABLE JEREMY D. PETERSON  
United States Magistrate Judge



Approved as to form by AUSA SAM STEFANKI

**ATTACHMENT A**

The property to be searched is the following electronic devices (collectively, the “Subject Devices”), all of which are currently located in a secure evidence facility at 2001 Freedom Way, Roseville, California 95678:

- a) One Apple iPhone in a blue case bearing an unknown serial number (“Subject Device 1”);
- b) One black Samsung LG cellular telephone bearing an unknown serial number (“Subject Device 2”);
- c) One silver Apple iPhone in a clear case bearing an unknown serial number (“Subject Device 3”);
- d) One black Samsung cellular telephone bearing an unknown serial number (“Subject Device 4”);
- e) One silver and white Samsung cellular telephone bearing an unknown serial number (“Subject Device 5”);
- f) One Microsoft Surface Pro tablet bearing serial number JT2L416JA1C (“Subject Device 6”); and
- g) One white Samsung cellular telephone bearing an unknown serial number (“Subject Device 7”).

This warrant authorizes the forensic examination of the Subject Devices for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

1. All records on the Subject Devices described in Attachment A that relate to violations of 21 U.S.C. §§ 846 and 841(a)(1) and involve Holly Adams and/or Devlin Hosner, including:

- a) Data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;
- b) Any and all documents, records, or information related to the access, creation, and maintenance of websites and hidden (Tor-based) services;
- c) Any and all documents records, or information relating to email accounts used in furtherance of the violations;
- d) Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;
- e) Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;
- f) Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;
- g) Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, Wickr, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;
- h) Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;
- i) Contents of any calendar or date book;

///



- j) Global Positioning System (“GPS”) coordinates and other information or records identifying travel routes, destinations, origination points, and other locations from December 1, 2020, to present.
2. With respect to any of the Subject Devices containing evidence falling within the scope of the foregoing categories of items to be seized:
- a) Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
  - b) Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c) Evidence of the attachment of other devices;
  - d) Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
  - e) Evidence of the times the device was used;
  - f) Passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;
  - g) Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
  - h) Records of or information about Internet Protocol addresses used by the device;
  - i) Records of or information about the device’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**ATTACHMENT C**



Case No.:

Copy of warrant and inventory left with:

Inventory of the property taken and name of any person(s) seized:

## Date: \_\_\_\_\_

---

Printed name and title

**AFFIDAVIT**

I, Christopher Scott Fitzpatrick, being duly sworn, declare and state as follows:

**I. PURPOSE OF AFFIDAVIT**

1. This affidavit is made in support of an application for a warrant to search the person of Devlin Takeoka HOSNER ("HOSNER") as described more fully in Attachment A-1, the person Holly Danielle ADAMS ("ADAMS") as described in more fully in Attachment A-2, a 2020 Toyota Prius bearing California license plate number 8NDG907 (the "SUBJECT VEHICLE") as described more fully in Attachment A-3, and Room #224 at the Indian Wells Resort Hotel, located at 76661 Palmeras Road, CA-111, Indian Wells, California 92210 (the "SUBJECT PREMISES") as described more fully in Attachment A-4.

2. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), as described more fully in Attachment B. Attachments A-1, A-2, A-3, A-4, and B are incorporated herein by reference.

3. The applied-for search warrants would authorize the forensic examination of any electronic devices seized pursuant to the search warrants to identify electronically stored data particularly described in Attachment B.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and

information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

## **II. BACKGROUND OF AFFIANT**

5. I am a Special Agent of the Department of Treasury, Internal Revenue Service - Criminal Investigation ("IRS-CI") since September 2001. I am currently assigned to the IRS-CI Sacramento Office, and I am charged with investigating drug trafficking and money laundering activities in the Eastern District of California, and elsewhere. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and I am empowered by law to conduct investigations and make arrests for federal felony offenses. Additionally, I am a federal law enforcement officer within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure, that is, a federal law enforcement agent engaged in enforcing criminal laws and authorized to request a search warrant.

6. I was trained at the Federal Law Enforcement Training Center located in Glynco, Georgia. During my training, I received special training in money laundering, including but not limited to, 18 U.S.C. § 1957 and 31 U.S.C. § 5324(a)(1). I also received special training in specified unlawful activities under

the money laundering statutes, including but not limited to, violations of 21 U.S.C. §§ 846 and 841(a)(1). I have also spoken to and worked with experienced federal, state, and municipal agents and narcotics officers regarding the methods and means employed by drug manufacturers and drug traffickers, including their use of express carriers and the USPS to distribute illegal narcotics.

7. During the course of my employment as an IRS-CI Special Agent, I have participated in numerous criminal investigations. I have participated in executing numerous Federal and State search warrants involving the aforementioned listed controlled substances, the seizure of narcotics-related records and other types of evidence that document the activities of criminal organizations in both the manufacturing and distribution of controlled substances, and the money laundering of the criminally derived proceeds. To successfully conduct these investigations, I have utilized a variety of investigative techniques and resources, including physical and electronic surveillance, various types of infiltration, including undercover agents, informants, and cooperating sources. Through these investigations, my training and experience, and conversations with other agents and law enforcement personnel, I am familiar with the methods used by drug traffickers to smuggle and safeguard controlled substances, to distribute, manufacture, and transport controlled substances, and to collect and launder related proceeds.

8. I am part of the Northern California Illicit Digital Economy ("NCIDE") task force composed of IRS-CI, Homeland Security Investigations ("HSI"), the Federal Bureau of Investigation ("FBI"), the United States Postal Inspection Service ("USPIS"), the United States Postal Inspection Service-Office of the Inspector General ("USPIS-OIG"), and the Drug Enforcement Administration ("DEA"). As a function of this task force, investigators regularly purchase narcotics utilizing both digital and fiat currencies, from the persons operating and illegally selling narcotics on the "clear" portion of the internet, from the "dark" portion of the internet and from various social media platforms. Investigators conduct the undercover purchases of narcotics to assist in the effort to identify the suspects operating such illicit sites.

### **III. TECHNICAL TERMS**

9. Pretty Good Privacy ("PGP") is an encryption program that provides cryptographic privacy and authentication for data communication. PGP makes use of public-key encryption, in which one key is used to encrypt the data (the public key) and another key is used to decrypt it (the private key). This technology allows, for example, a dark-web drug vendor to communicate in an encrypted format by broadcasting his/her public key to customers who can then encrypt messages they want to send to the vendor.

10. Digital currency (also known as cryptocurrency) is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (fiat currency is created and regulated by a government).



11. Digital currency exists entirely on the internet and is not stored in any physical form. Digital currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Digital currency is not illegal in the United States and may be used for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions, such as the sale of controlled substances.

12. Bitcoin is a type of digital currency. Bitcoin payments are recorded in a public ledger that is maintained by peer-to-peer verification and is thus not managed by a single administrator or entity.

13. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be done on any type of computer, including laptop computers and smart phones.

14. Bitcoins can be stored in digital "wallets." A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access Bitcoins on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to an account number, while the private key is like the password to access that account.

15. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true

identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

16. The dark web, or darknet, consists of websites accessible only through encrypted means. Using the dark web, individuals have established online marketplaces, such as Silk Road, for narcotics and other illegal items. These markets often only accept payment through digital currencies, such as Bitcoin. Accordingly, a large number of Bitcoin sales or purchases by an individual often indicate that the individual is involved in narcotics trafficking or the distribution of other illegal items. Individuals intending to purchase illegal items on Silk Road-like websites need to purchase or barter for Bitcoins. Further, individuals who receive Bitcoin as proceeds of illegal sales on Silk Road-like websites need to sell their Bitcoin to convert them to fiat currency. Such purchases and sales are often facilitated by peer-to-peer Bitcoin exchangers who advertise their services on websites designed to facilitate such transactions.

17. Dark web sites, such as Silk Road, AlphaBay, Empire, Dark0de, and ToRReZ, operate on "The Onion Router" or "Tor" network. The Tor network ("Tor") is a special network of computers on the internet, distributed around the world, that is designed to conceal the true Internet Protocol ("IP") addresses

of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such "hidden services" operating on Tor have complex web addresses, which are many times generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software designed to access the Tor network.

#### **IV. SUMMARY OF PROBABLE CAUSE**

18. Since at least in or around May 2021, law enforcement agents have been investigating HOSNER and ADAMS for running an illegal narcotics distribution operation on various encrypted websites on the dark web. During this investigation, law enforcement officers conducted multiple undercover purchases of counterfeit oxycodone pills from HOSNER and ADAMS that contain fentanyl. Agents also observed ADAMS place a parcel containing illegal narcotics into the mail using a facility maintained by the United States Postal Service ("USPS"). Additionally, agents traced monies used in undercover narcotics purchases to financial accounts controlled by HOSNER, and agents also reviewed structured cash withdrawals made by HOSNER that appear designed to evade financial reporting requirements imposed by federal law.

19. During this federal investigation, state and local law enforcement officers executed search warrants at locations

associated with HOSNER and ADAMS. Officers recovered additional amounts of illegal narcotics that also contained fentanyl, firearms, and other contraband during execution of these non-federal search warrants.

20. According to California Department of Motor Vehicle records, ADAMS is registered owner of the SUBJECT VEHICLE.

21. Finally, though HOSNER and ADAMS are transient, hotel records show, and our surveillance has confirmed, that HOSNER and ADAMS are staying at the SUBJECT PREMISES and have rented the SUBJECT PREMISES through March 31, 2022.

#### **V. STATEMENT OF PROBABLE CAUSE**

##### **a. Initiation of Investigation Into Dark Web Vendor "IGOGRRAAWWR."**

22. On or around May 2, 2021, the NCIDE Task Force opened a joint investigation of a user identifying themselves as "IGOGRRAAWWR," a dark web vendor suspected of mailing controlled substances via the USPS. IGOGRRAAWWR offered products for sale via a vendor site on a dark web marketplace for illicit sales known as ToRReZ. IGOGRRAAWWR created an account on the ToRReZ marketplace on or around December 27, 2020.

23. IGOGRRAAWWR's listings described pills they were selling as "strong as fuck" and advised buyers to be careful. In my training and experience, the wording of these listings suggests that the pills contained a controlled substance. IGOGRRAAWWR's vendor site offered customers various quantities of counterfeit pressed oxycodone pills and stolen credit card information.

**b. IGOGRRAAWWR Is Connected to ADAMS and HOSNER.**

24. The PGP public key associated to IGOGRRAAWWR on ToRReZ listed grraawwr76@gmail.com as IGOGRRAAWWR's email address.<sup>1</sup> Agents conducted online research of open-source information for the term "grraawwr76" and found the existence of a user account on the adult website manyvids.com with the username "Grraawwr76" and a profile image.

25. When I searched online sources for that e-mail address, the name Holly Danielle Adams appeared online.

26. Once I received that name, I ran the name through the California Department of Motor Vehicle ("DMV") database and retrieved the photograph for ADAMS.

27. I then compared a photograph of ADAMS maintained by the DMV to the profile image of the "grrawwr76" user account on manyvids.com. In my opinion, these two images are both of ADAMS. The persons depicted in the DMV photo and the grraawwr76-manyvids.com-profile are white women with red hair and distinct facial characteristics.

28. On May 2, 2021, a member of the NCIDE Task Force, operating in an undercover capacity, conducted a purchase of 200 counterfeit oxycodone pills from IGOGRRAAWWR on the ToRReZ marketplace. On May 6, 2021, the parcel was delivered to an address controlled by law enforcement in the Eastern District of California. The return address on the parcel purported to be from an individual named Danielle Rivera, with a contact phone

---

<sup>1</sup> PGP public keys are bound to a user-submitted email address.

number of 760-777-2839. Records maintained by the USPS for telephone number 760-777-2839 contain an account registered in the name of "Amanda Hensley" at an address on Avenida Ramirez in La Quinta, California.

29. California DMV records contain information for an Amanda Hensley, with a date of birth of May 13, 19XX.<sup>2</sup> I conducted a search of Thomson Reuters CLEAR, a paid subscription of public and proprietary records online database, for "Amanda Hensley with the date of birth May 13, 19XX." This search revealed that Amanda Hensley's most recent address was 80866 Brown Street, Indio, California 92201. I conducted a subsequent search of CLEAR for this address, which revealed that both ADAMS and HOSNER had received packages at this address.

30. I then ran a criminal history check of HOSNER and saw that he had a history of identity theft and narcotics convictions.

31. Based on the postal address research above, I conducted a search for information related to HOSNER on open-source social media platforms. My search revealed an Instagram account with the handle "devlinhosner." This Instagram account had zero posts. However, the "devlinhosner" account was following an Instagram account with the handle "hollygrraawwr." The "hollygrraawwr" account was the only other Instagram account being followed by the "devlinhosner" account at the time.

---

<sup>2</sup> Based on ADAMS's California Driver's License, I know that ADAMS's true date of birth is May 13, but in a different year than the year Amanda Hensley was born. While ADAMS's precise birth year is known to me, I have omitted it here because it would constitute personally identifiable information.

Agents concluded that the "grraawwr" username was sufficiently unusual and similar to the manyvids.com and ToRReZ usernames to conduct additional open-source research on HOSNER and ADAMS.

32. I reviewed publicly available images posted by the owner of the "hollygrraawwr" Instagram account, and these images suggest that ADAMS and HOSNER are romantically involved. Furthermore, images posted to the "hollygrraawwr" Instagram account's photo album contained some of the same images as the "grraawwr76" account on manyvids.com.

33. The "hollygrrawwr" Instagram account also displayed multiple photographs of a recognizable dog that appeared to belong to the owner of the "hollygrrawwr" Instagram account. The "hollygrrawwr" Instagram account contained various hashtags appeared to be related to the owner's dog, including the hashtag "lilination." I recognized this dog to be the same animal displayed in images on the "igogrraawwr" vendor page on the ToRReZ marketplace.

**c. Law Enforcement Conducted Multiple Undercover Purchases of Illegal Narcotics From IGOGRAAWWR.**

34. Between May and September of 2021, NCIDE Task Force agents conducted at least four separate undercover purchases of counterfeit oxycodone pills from IGOGRAAWWR. All of these undercover purchases occurred on the ToRReZ marketplace as follows:

Order date	Items ordered	Payment	Delivery date to EDCA	Testing status
May 2, 2021	200 counterfeit oxycodone pills	\$1,015 in Bitcoin	May 6, 2021	pending
May 31, 2021	35 counterfeit oxycodone pills	\$360 in Bitcoin	June 7, 2021	Positive for fentanyl

July 19, 2021	10 counterfeit oxycodone pills	\$130 in Bitcoin	July 19, 2021	Positive for fentanyl
Sept. 2, 2021	300 counterfeit oxycodone pills	\$1,620 in Bitcoin	Sept. 10, 2021	Positive for fentanyl

35. Postal Service records show that the May 31, 2021, package was sent from a post office in La Quinta, California. Surveillance video from this post office captured ADAMS mailing a package on June 2, 2021.

**d. ADAMS and HOSNER Used a Shipping Services Website to Send Hundreds of Packages Between May and September of 2021.**

36. Shipping Company 1 is a company that helps e-commerce businesses compare shipping rates; create shipping labels; ship packages through various shipping companies, including the USPS, United Parcel Service, Federal Express, and DHL; and track packages. Shipping Company 1 charges their customers a fee for this service.

37. Based on agents' analysis of HOSNER's connection with ADAMS, the IGOGRAAWWR username, and records obtained from Coinbase (see below) agents served legal Process on JPMorgan Chase Bank NA. From JPMorgan, agents learned that<sup>3</sup> HOSNER opened a checking account with JPMorgan Chase Bank NA in or around the summer of 2020. I obtained and reviewed records from this financial institution relating to HOSNER's account. Between June 5, 2021, and August 5, 2021, HOSNER's account made approximately eighty payments to Shipping Company 1 totaling approximately \$8,600.

---

<sup>3</sup> Agents served legal process on multiple financial institutions to determine whether these individuals had accounts.



38. According to records provided to me by Shipping Company 1, on May 5, 2021, a customer associated with the email account amandahensley513@gmail.com created an account with Shipping Company 1. Shipping Company 1 does not require an individual seeking to open an account to provide their first and last name.

39. According to records provided to me by Shipping Company 1, between May 10, 2021, and September 8, 2021, the account associated with amandahensley513@gmail.com shipped approximately 1,150 packages. The packages were mailed to various individuals located all over the United States. As a result of my training and experience, I know that darkweb drug vendors transport their products through the United States Postal Service. The number of packages mailed by the [amandahensley513@gmail.com](mailto:amandahensley513@gmail.com) account (1,150), and number of payments paid by HOSNER to Shipping Company 1 (80), and the total volume of payments by HOSNER to Shipping Company 1 (\$8,600) is consistent with the volume of shipments believed to be sold by IGOGRAAWWR on darkweb marketplaces.

40. According to records provided to me by Shipping Company 1, Shipping Company 1 charged the account associated with amandahensley513@gmail.com to ship the four undercover purchases of illegal narcotics by law enforcement from IGOGRRAAWWR described previously in this affidavit.

**e. HOSNER Used His Coinbase, PayPal, and JPMorgan Chase Accounts to Launder Bitcoin Received on the Dark Web by Converting It to Fiat Currency.**

41. Based on agents' analysis regarding HOSNER's connection with ADAMS and the IGOGRAAWWR username, agents served legal Process on Coinbase. Coinbase is a popular online cryptocurrency exchange where individuals can purchase or sell various types of cryptocurrencies, such as Bitcoin and Ethereum. Based on my training and experience investigating dark web narcotic operations, dark web vendors often use cryptocurrency exchange companies such as Coinbase to cash out their illicit and fraudulently obtained proceeds. Doing so allows criminal to convert ill-gotten proceeds to fiat currency.

42. PayPal is a company that offers an online financial service that allows users to transfer fiat currency between accounts electronically. JPMorgan Chase is a traditional brick-and-mortar bank.

**1. HOSNER Used His Coinbase Account to Convert Bitcoin to Fiat Currency.**

43. According to Coinbase records, HOSNER opened a Coinbase account on or around March 31, 2021. Between April 29, 2021, and August 15, 2021 (which is the most recent date for which law enforcement has records relating to HOSNER's Coinbase account), HOSNER sold in excess of \$800,000 worth of Bitcoin and converted the Bitcoin to dollars.

44. An FBI analyst reviewed HOSNER's Coinbase account for evidence of illegal activity. Using a proprietary blockchain investigative tool, the analyst traced 1.7902 Bitcoin, which

totalled \$71,213.02 out of the approximately \$800,000 worth of Bitcoin that was deposited into HOSNER's Coinbase account during the investigative time period. The FBI analyst concluded that the Bitcoin deposits into HOSNER's Coinbase account originated from the ToRReZ and World Market marketplaces.<sup>4</sup> Both of these marketplaces are located on the dark web and only exist to sell illegal narcotics and other contraband. Furthermore, during the investigation, agents routinely observed IGOGRRAAWWR's vendor account on ToRReZ. At no time did IGOGRRAAWWR offer to sell anything that was not contraband.

45. Based on my training and experience and on facts I know from this investigation, I believe that all or most of the \$71,213.02 worth of Bitcoin deposited into HOSNER's Coinbase account consists of proceeds of illegal drug trafficking paid to IGOGRRAAWWR.

**f. ADAMS and HOSNER Continue to Distribute Narcotics Under Alternative Dark Web Identities "grrraawwr760" and "ITS4REAL."**

46. On or around September 8, 2021, ADAMS and HOSNER were arrested by local law enforcement.<sup>5</sup> Following this arrest, a member of the NCIDE Task Force operating undercover used an encrypted messaging application known as Wickr to contact an

---

<sup>4</sup>The FBI analysis revealed the traced Bitcoin (1.7902 Bitcoin, totaling \$71,213.02) was a one-hop transaction from one wallet address associated to a dark web marketplace to wallet address belonging to HOSNER.

<sup>5</sup> The local arrest of ADAMS and HOSNER were unrelated to this federal drug investigation. The local arresting officers were responding to a citizen complaint regarding activity at HOSNER's location, which resulted in the execution of a state search warrant. This affidavit does reply on the fruits of that search or arrest.

account on Wickr ("grraawwr760") that IGOGRRAAWWR previously used to communicate regarding narcotics orders placed on its dark web vendor accounts.

47. On December 9, 2021, the undercover agent sent a message on Wickr to "grraawwr760" asking if they were back in business. Several hours later, the undercover agent received a reply from "grraawwr760." In the ensuing conversation, "grraawwr760" confirmed their identity as IGOGRRAAWWR by providing the surname previously used by the undercover agent in that agent's prior undercover purchases from IGOGRAAWWR. In the same conversation, "grraawwr760" indicated that they were absent from dark web vending because they "had to deal with old warrants and that's why I was Mia for a min." "grraawwr760" also stated, "But been bk for a couple months but again only on here to select ppl who have ordered from me a decent amount of times, my top top regulars."

48. "grraawwr760" then confirmed that they were going to re-supply their narcotics the next day and informed the undercover agent that "grraawwr" would fill new orders if the undercover agent wanted to purchase any counterfeit oxycodone. "grraawwr760" said of the pills, "Do u snort or smoke them? (They're good for either way) if u snort them, my ppl who also snort tell me these are great because 1 potency and 2 they break down easier, like not so hard to crush. Lol If u smoke them then they have the super popcorn taste and when smoked on foil give the golden trails[.]"

49. The undercover agent inquired if "grraawwr760" was going to operate on a marketplace again, to which they replied, "Nah. I don't want to be open to new customers just regulars[.]" The undercover agent requested a photo of the counterfeit oxycodone that "grraawwr760" was offering to sell. On or about December 11, 2021, "grraawwr760" sent a photograph of the pills held in an open hand. "Grraawwr760" also provided a Bitcoin address for payment. The undercover agent did not finalize a purchase at the time.

50. On or around January 29, 2022, the undercover agent received a message on Wickr from "grraawwr760" with a link to the Dark0de marketplace profile of a vendor with the name "ITS4REAL" and the message, "This may or may not be me hehe[.]" "grraawwr760" also stated, "also always welcome to do direct deals with me. The new profile is a collaboration, so it's me working with a few ppl in a group instead of me running it solo[.]"

51. Agents conducted additional online purchases of counterfeit oxycodone pills from "grraawwr760" on or around January 30, 2022; February 2, 2022, February 8, 2022, February 21, 2022, March 1, 2022, and March 9, 2022. In each case, the order was followed by the delivery of pills to the undercover address in the Eastern District of California.

52. On or around February 14, 2022, "grraawwr760" notified the undercover agent that, "I got the release thanks so much! Glad to do biz with u!!" The undercover agent replied by complimenting "grraawwr760" on the decoys used in their packages

to hide narcotics. The undercover agent also commented on the photograph that "grraawwr760" had added to their Wickr profile. This photograph is of the same dog from ADAMS's Instagram account describe earlier in this affidavit. "grraawwr760" replied, "She's a chow chow chihuahua I got her doggy DNA done lol[.]" When asked about the dog's name, "grraawwr760" replied, "Lili (Lee lee)."

53. On or around March 10, 2020, "grraawwr760" replied to the undercover agent's statement about the comparative strength of the pills stating, "Usually there supposed to be pressed with fentanyl and that's what's in mine, hers are some fake weak shit."

**g. Investigation of the SUBJECT VEHICLE**

54. Based on my training and experience, persons engaged in drug trafficking often maintain drugs in their personal vehicles. There are many reasons why persons engaged in drug trafficking maintain drugs in their vehicles. Drug traffickers are concerned that law enforcement will search their residence, so they store the drugs in their vehicle. Often the drugs are hidden in false compartments within the vehicle. Drugs can also be hidden in an engine part such as an air filter that wouldn't be searched. Furthermore, I know that dark web drug vendors use varied U.S. Postal Service facilities to mail the ordered drugs to their customers.

55. According to DMV records, ADAMS is the registered owner of a white, 2020 model year Toyota Prius, bearing California license plate 8NDG907 and Vehicle Identification

Number ("VIN") JTDKARFP9L3139481 (the SUBJECT VEHICLE), which is registered to ADAMS at 43100 Palm Royal Drive, Apt. #313, La Quinta, California 92253. According to publicly placed license-plate readers, as of March 20, 2022, the SUBJECT VEHICLE has traveled on highways in the general area of Indian Wells, California, Palm Desert, California, and Rancho Mirage, California.

56. There is probable cause to believe that ADAMS is using the SUBJECT VEHICLE to mail the undercover purchases made by law enforcement and by other customers. As stated above, on or around February 8, 2022, a member of the NCIDE Task Force purchased 150 pressed m30s (counterfeit oxycodone) pills from ITS4REAL on the Dark0de marketplace other narcotic purchases by other customers. On February 11, 2021, the parcel containing the suspected narcotics was mailed from the Palm Desert, California, post office. Furthermore, there is probable cause to believe that based upon the different geographic locations from which the undercover purchases were made, a mode of vehicle transportation was utilized.

57. On March 25, 2022, a federal agent saw the SUBJECT VEHICLE at a hotel in which ADAMS and HOSNER were staying. On March 26, 2022, a local law enforcement officer saw the SUBJECT VEHICLE in the parking lot pertaining to the SUBJECT PREMESIS (see further description below). On March 27, 2022, a federal agent saw the SUBJECT VEHICLE in the parking lot pertaining to the SUBJECT PREMESIS. As a result, I believe that ADAMS and HOSNER moved their belongings from the former hotel to the

current hotel using the SUBJECT VEHICLE, and therefore evidence of their crimes was likely transported, and may still remain, in that car.

58. Based on the forgoing, there is probable cause to believe evidence of the Subject Offenses will be located in the SUBJECT VEHICLE.

**h. Investigation of the SUBJECT PREMISES**

59. The investigation into both HOSNER and ADAMS has revealed they are both very transient and there is no known apartment or house where they reside. Moreover, the investigation revealed that both HOSNER and ADAMS move from one place to the next, often times renting Airbnb locations and hotel rooms. For example, according to Inn at Deep Canyon records, between March 15, 2022, and March 24, 2022, and checked out on March 25, 2022, HOSNER rented hotel room #106 located at 74470 Abronia Trail, Palm Desert, California. According to Inn at Deep Canyon records, a debit card in ADAMS's name paid for the hotel stay.

60. On March 23, 2022, and March 24, 2022, law enforcement saw the SUBEJCT VEHICLE parked in the parking lot of the Inn at Deep Canyon. Furthermore, on March 24, 2022, law enforcement saw HOSNER and a female believed to be ADAMS taking a small dog<sup>6</sup> to the lawn. After the dog was taken to the lawn, HOSNER and the female believed to be ADAMS entered hotel room #106.

---

<sup>6</sup> The small dog appeared to be the same dog observed in photographs on ADAMS's Instagram account under the handle "hollygrrawwr."



61. According to an employee at the Inn at Deep Canyon, on March 24, 2022, a maintenance person entered hotel room #106 because there was a plumbing issue in room #108. Other than this contact, the occupants of room #106 did not allow housekeeping to enter the room. While inside hotel room #106, the maintenance person said the occupants of hotel room #106 looked like people who used heroin.<sup>7</sup> The maintenance person said it appeared the four occupants—two men and two women—inside the hotel room were making credit cards<sup>8</sup> with a printer and looked like a swap meet with bags and items laid out. As set forth above, the undercover buys made by law enforcement contained miscellaneous bags and items to disguise the drugs.

62. On March 26, 2022, agents saw the SUBJECT VEHICLE parked in the parking lot of the Indian Wells Resort Hotel, located at 76661 Palمرas Road, CA-111, Indian Wells, California 92210. Agents again saw the SUBJECT VEHICLE at the same hotel on March 27, 2022.

63. On March 27, 2022, agents requested a list of guests that had recently checked in from management at the Indian Wells Resort Hotel. On the list, agents saw that HOSNER checked into room 224 (the SUBJECT PREMISES) on March 24, 2022, and reserved the room through March 31, 2022. Surveilling agents also

---

<sup>7</sup> The maintenance worker did not provide more specific information, but his opinion is recounted here for the value of noting that an ordinary person might suspect that drug and criminal activities were occurring in the room even after just a quick look in the room.

<sup>8</sup> As set forth above, the vendor "IGOGRRRAWWR" on the TORReZ marketplace sold stolen credit card information.

observed an unidentified woman walking a dog appearing to be the same dog described above. The agent asked the woman the dog's name, and the woman (who was not ADAMS) responded "LiLi." The woman then walked to the floor on which room 224 is located, but the agent did not follow her to the room to avoid arousing suspicion. The presence of the woman is consistent with the previous hotel staff's description of another female staying in the room with ADAMS and HOSNER. Later, an agent saw the exact location of room 224 and found that the "Do Not Disturb" sign had been taped to the door, which is consistent with the occupants' behavior at the previous hotel.

64. Based on the forgoing, there is probable cause to believe evidence of the Subject Offenses will be located in the SUBJECT PREMISES.

**i. Evidence Expected to Seize from HOSNER's Person and ADAMS's Person, the SUBJECT VEHICLE, and from the SUBJECT PREMISES**

65. There is probable cause to believe that evidence of the Subject Offenses will be seized from HOSNER's person, ADAMS' person and from the SUBJECT VEHICLE, including:

- a. Controlled substances, including pressed counterfeit oxycodone;
- b. Packaging, mylar bags, and other personal items to conceal the controlled substances;
- c. Records reflecting the mailing or receipt of packages through Express mail, Priority Mail, United Parcel Service or any other common carrier;

d. Documents, records or information relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of a controlled substance;

e. Documents, records or information relating to the transfer, purchase, sale or disposition of virtual currency;

f. Documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services;

g. Documents, records, information relating to email accounts used in furtherance of these offenses;

h. Efforts to avoid detection by law enforcement;  
and

i. Bank records, checks, credit card bills, account information, and other financial records.

#### **VI. TRAINING AND EXPERIENCE ON DRUG OFFENSES**

66. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their

vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

**VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES<sup>9</sup>**

67. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

---

<sup>9</sup> As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

68. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

69. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a



device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress HOSNER's and ADAMS's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of HOSNER's and ADAMS's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

#### **VIII. CONCLUSION**

70. For all of the reasons described above, there is probable cause to believe that HOSNER and ADAMS have committed violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances).

There is also probable cause that the items to be seized described in Attachment B will be found in a search of HOSNER's person, ADAMS's person, the SUBJECT VEHICLE, and the SUBJECT PREMISES, as described in Attachments A-1 through A-4.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 29<sup>th</sup> day of March, 2022.

A handwritten signature in black ink, appearing to read "Kenby Mc", written over a horizontal line.

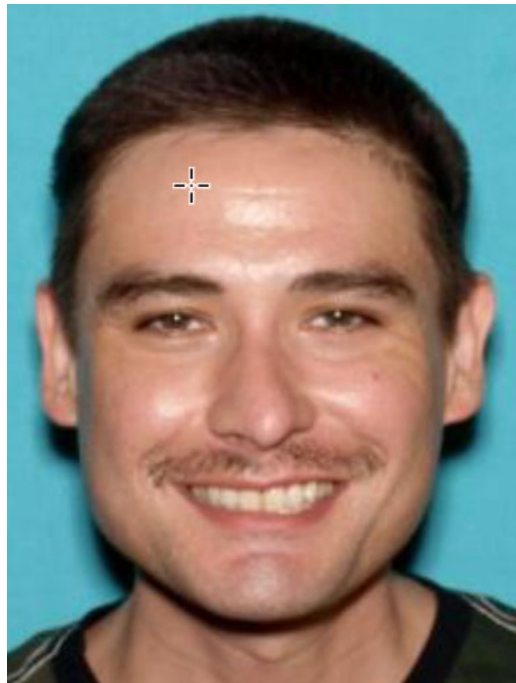
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A-1**

PERSON TO BE SEARCHED

The person of Devlin Takeoka HOSNER ("HOSNER"), date of birth January 8, 1989, with California Driver's License Number D7569343. HOSNER's California Department of Motor Vehicle records list him as standing 5'8" tall with brown hair and brown eyes. HOSNER is depicted in the photograph below.

The search of HOSNER shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within HOSNER's immediate vicinity and control at the location where the search warrant is executed.



**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) (the "Subject Offenses"), namely:

a. Any controlled substance, controlled substance analogue, or listed chemical;

b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;

c. Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

d. United States currency over \$1,000 or bearer instruments worth over \$1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first \$1,000), and data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or

transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;

e. Any and all documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services;

f. Any and all documents, records, or information relating to email accounts used in furtherance of the violations;

g. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

h. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

i. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to

show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

j. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, Wickr, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

k. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

l. Contents of any calendar or date book;

m. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations from December 1, 2020, to present; and

n. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

o. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries,

configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

## **II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)**

4. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or



seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or

evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel

assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

1. During the execution of this search warrant, law enforcement is permitted to: (1) depress HOSNER's and ADAMS's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of HOSNER's or ADAMS's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, [490 U.S. 386](#) (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of )  
One Apple iPhone in a blue case bearing an unknown )  
serial number; )  
One black Samsung LG cellular telephone bearing an )  
unknown serial number; )  
One silver Apple iPhone in a clear case bearing an )  
unknown serial number; )  
One black Samsung cellular telephone bearing an )  
unknown serial number; )  
One silver and white Samsung cellular telephone )  
bearing an unknown serial number; )  
One Microsoft Surface Pro tablet bearing serial )  
number JT2L416JA1C; and )  
One white Samsung cellular telephone bearing an )  
unknown serial number; )  
CURRENTLY LOCATED AT 2001 Freedom Way, )  
Roseville, California 95678 )

Case No. 2:22-sw-523-JDP

**SEARCH AND SEIZURE WARRANT**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ Eastern \_\_\_\_\_ District of \_\_\_\_\_ California \_\_\_\_\_  
(*identify the person or describe the property to be searched and give its location*):

**SEE ATTACHMENT A, attached hereto and incorporated by reference.**

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (*identify the person or describe the property to be seized*):

**SEE ATTACHMENT B, attached hereto and incorporated by reference.**

**YOU ARE COMMANDED** to execute this warrant on or before \_\_\_\_\_ August 19, 2022 \_\_\_\_\_ (*not to exceed 14 days*)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory

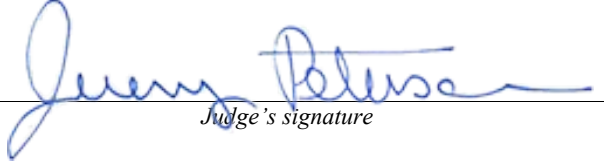
as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for \_\_\_\_\_ days (*not to exceed 30*)    ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: August 5, 2022 at 11:33 a.m.

City and state: Sacramento, California

  
\_\_\_\_\_  
*Judge's signature*

\_\_\_\_\_  
Jeremy D. Peterson, U.S. Magistrate Judge  
*Printed name and title*

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:                    		
Certification		
<p>I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.</p> <p style="text-align: center;">_____</p> <p style="text-align: center;">Subscribed, sworn to, and returned before me this date.</p> <p style="text-align: center;">_____</p> <div><div>_____ Signature of Judge</div><div>_____ Date</div></div>		

**ATTACHMENT A**

The property to be searched is the following electronic devices (collectively, the “Subject Devices”), all of which are currently located in a secure evidence facility at 2001 Freedom Way, Roseville, California 95678:

- a) One Apple iPhone in a blue case bearing an unknown serial number (“Subject Device 1”);
- b) One black Samsung LG cellular telephone bearing an unknown serial number (“Subject Device 2”);
- c) One silver Apple iPhone in a clear case bearing an unknown serial number (“Subject Device 3”);
- d) One black Samsung cellular telephone bearing an unknown serial number (“Subject Device 4”);
- e) One silver and white Samsung cellular telephone bearing an unknown serial number (“Subject Device 5”);
- f) One Microsoft Surface Pro tablet bearing serial number JT2L416JA1C (“Subject Device 6”); and
- g) One white Samsung cellular telephone bearing an unknown serial number (“Subject Device 7”).

This warrant authorizes the forensic examination of the Subject Devices for the purpose of identifying the electronically stored information described in Attachment B.



**ATTACHMENT B**

1. All records on the Subject Devices described in Attachment A that relate to violations of 21 U.S.C. §§ 846 and 841(a)(1) and involve Holly Adams and/or Devlin Hosner, including:

- a) Data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;
- b) Any and all documents, records, or information related to the access, creation, and maintenance of websites and hidden (Tor-based) services;
- c) Any and all documents records, or information relating to email accounts used in furtherance of the violations;
- d) Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;
- e) Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;
- f) Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;
- g) Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, Wickr, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;
- h) Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;
- i) Contents of any calendar or date book;

///

- j) Global Positioning System (“GPS”) coordinates and other information or records identifying travel routes, destinations, origination points, and other locations from December 1, 2020, to present.
2. With respect to any of the Subject Devices containing evidence falling within the scope of the foregoing categories of items to be seized:
- a) Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
  - b) Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c) Evidence of the attachment of other devices;
  - d) Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
  - e) Evidence of the times the device was used;
  - f) Passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;
  - g) Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
  - h) Records of or information about Internet Protocol addresses used by the device;
  - i) Records of or information about the device’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.